C L A I M S

1. (currently amended) A method for forwarding messages in a multi-node network comprising decrypting, by any forwarding node, any message received by said any forwarding node and encrypting each message transmitted by said any forwarding node.

2. (cancelled)

3. (previously presented) The method of claim 2, wherein said decrypting and said encrypting are carried out using symmetrical encryption and decryption.

4. (previously presented) The method of claim 2, wherein said decrypting and said encrypting are carried out using asymmetric encryption and decryption.

5. (currently amended) A method for forwarding messages in a multi-node network comprising decrypting, by any forwarding node, any message received by said any forwarding node prior to determining a destination for said received message and encrypting, by said any forwarding node, each message transmitted by said any forwarding node.

6. (cancelled)

7. (original) The method of claim 6, wherein said decrypting and said encrypting are carried out using a symmetrical encryption and decryption algorithm.

8. (original) The method of claim 6, wherein said decrypting and said encrypting are carried out using an asymmetric encryption and decryption algorithm.

9. (previously presented) A method for encrypting and decrypting messages in a multi-node network, comprising:

(a)   encrypting a message by a source node and transmitting said encrypted message to any forwarding node;

(b)   receiving and decrypting said encrypted message by said any forwarding node;

(c)   re-encrypting said decrypted message by said any forwarding node and transmitting said re-encrypted message to a destination node; and

(d)   receiving and decrypting said re-encrypted message by said destination node.

10. (previously presented) The method of claim 9, wherein said encrypting said message by said source node, said decrypting of said transmitted message by said any forwarding node, said re-encrypting of said decrypted message by said any forwarding node, and said decrypting of said re-encrypted message by said destination node, are carried out using symmetrical encryption and decryption.

11. (previously presented) The method of claim 10, wherein:

(a)   said encrypting said message by said source node is carried out using a first key;

(b)   said decrypting said re-encrypted message by said destination node is carried out using said first key;

(c)   said decrypting of said transmitted message by said any forwarding node is carried out using a second key; and

3

(d)   said re-encrypting of said decrypted message by said any forwarding node is carried out using said second key.

12. (original) The method of claim 11, wherein said second key is different from said first key.

13. (original) The method of claim 11, wherein said second key and said first key are the same.

14. (previously presented) The method of claim 9, wherein said encrypting said message by said source node, said decrypting of said transmitted message by said any forwarding node, said re-encrypting of said decrypted message by said any forwarding node, and said decrypting of said re-encrypted message by said destination node, are carried out using asymmetric encryption and decryption.

15. (previously presented) The method of claim 14, wherein:

(a)   said encrypting said message by said source node is carried out using a first encryption key;

(b)   said decrypting said re-encrypted message by said destination node is carried out using a first decryption key;

(c)   said decrypting of said transmitted message by said any forwarding node is carried out using a second decryption key; and

(d)   said re-encrypting of said decrypted message by said any forwarding node is carried out using said second encryption key.

4

16. (original) The method of claim 15, wherein said second encryption key is different from said first encryption key, and said second decryption key is different from said first decryption key.

17. (original) The method of claim 15, wherein said second encryption key is the same as said first encryption key, and said second decryption key is the same as said first decryption key.

Claim 18 (cancelled)

19. (previously presented) An encryption and decryption system for a multiple node network, comprising a plurality of nodes, with each of the plurality of nodes including means for decrypting all received messages, and means for encrypting all transmitted messages.

20. (previously presented) The encryption and decryption system of claim 19, further comprising at least one source node, said source node including means for encrypting messages and transmitting said encrypted messages to any of the plurality of nodes.

21. (previously presented) The encryption and decryption system of claim 20, further comprising at least one destination node, said destination node including means for decrypting messages transmitted by any of the plurality of nodes.

22. (previously presented) The encryption and decryption system of claim 21, wherein said means for encrypting messages by said source node, said means for decrypting messages in said destination node, said means for decrypting messages by any of the plurality of nodes, and said means for encrypting messages by any of the plurality of nodes comprises symmetrical encryption and decryption.

23. (previously presented) The encryption and decryption system of claim 21, wherein said means for encrypting messages by said source node, said means for decrypting messages in said destination node, said means for decrypting messages by any of the plurality of nodes, and said means for encrypting messages by any of the plurality of nodes comprises asymmetrical encryption and decryption.